PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

108-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°108	Fecha: 09-05-2024 Página: 4 de 7

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Hackers gestionan miles de tiendas web falsas: más de 850.000 tarjetas robadas		
Tipo de Ataque	Portal fraudulento	Abreviatura	PortalFrau
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G02
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Una creciente red de ciberdelincuencia, "BogusBazaar", ha robado datos de tarjetas de crédito de más de 850.000 compradores en línea, principalmente en Europa occidental y Estados Unidos, mediante la operación de decenas de miles de sitios web de comercio electrónico fraudulentos.

Los investigadores de seguridad estiman que desde 2021, los piratas informáticos han procesado más de 1 millón de pedidos falsos por un total de más de 50 millones de dólares.

2. DETALLES:

El grupo criminal atrae a las víctimas a tiendas online falsas, utilizando a menudo dominios caducados que anteriormente tenían buenas clasificaciones en Google.

A partir de ahí, una vez han creado la web con ese dominio falso, van a simular que venden productos a precio muy bajo. Principalmente, van a vender zapatos y ropa de vestir. Lo que buscan es que la víctima haga una compra y, de esta forma, robar los datos de tarjeta. Esas páginas van a ser independientes, con un nombre y logo creados para dar una buena apariencia.

En lugar de gestionar directamente las más de 75.000 tiendas falsas, BogusBazaar funciona como una "franquicia" criminal:

Un equipo central gestiona la infraestructura técnica, incluida la implementación de tiendas falsas ya preparadas utilizando complementos personalizados de WordPress y WooCommerce.

Una red descentralizada de "afiliados", que se cree que tiene su sede principalmente en China, maneja las operaciones diarias de las tiendas falsas.

Los investigadores de seguridad descubrieron que cada servidor de BogusBazaar suele alojar alrededor de 200 tiendas falsas. Las presencias públicas de las tiendas están protegidas detrás de Cloudflare, mientras que los pagos se procesan a través de pasarelas como PayPal y Stripe.

Con el tiempo, los delincuentes han desarrollado una automatización sofisticada para establecer rápidamente nuevos escaparates e intercambiar páginas de pago para evadir la detección y los ataques. Esta agilidad técnica ha permitido que la red de fraude opere sin obstáculos durante años.

Los hallazgos se han compartido con las autoridades pertinentes y algunas tiendas de BogusBazaar ya están fuera de línea.

3. RECOMENDACIONES:

- No hacer clic en enlaces sospechosos o no solicitados. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Comunicarse directamente con la empresa, si recibe una solicitud inesperada de información personal, utilizando un número de teléfono o una dirección de correo electrónico desde su sitio web oficial.
- Utilizar software de seguridad. Proteger sus dispositivos con software antivirus actualizado, que puede ayudar a detectar y bloquear descargas y sitios maliciosos.
- Utilizar tarjetas secundarias. Se puede usar una exclusiva para las compras online y recargarla sólo con la cantidad que se vaya a necesitar. De esta forma, en caso de que ocurra un robo de datos, no podrían quitar tanto dinero de dicha cuenta bancaria.
- Realizar capacitaciones periódicas para dos grupos: los usuarios finales y su equipo de seguridad.

Fuente de Información:	• hxxps://gbhackers.com/alert-hackers-fake-webshops/ • hxxps://www.redeszone.net/noticias/seguridad/robo-miles-tarjetas-bancarias-internet/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°108	Fecha: 09-05-2024 Página: 5 de 7

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en F5 BIG-IP Next Central Manager API		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo inyección y validación de certificado inadecuada en F5 BIG-IP Next Central Manager API. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos y realizar un ataque MitM.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-26026 de tipo inyección SQL, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos. La vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario dentro de la API. Un atacante remoto no autenticado puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto leer, eliminar, modificar datos en la base de datos y obtener control total sobre la aplicación afectada.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-21793 de tipo inyección SQL, podría permitir a un atacante remoto ejecutar consultas SQL arbitrarias en la base de datos. La vulnerabilidad existe debido a una limpieza insuficiente de los datos proporcionados por el usuario dentro de la interfaz API. Un atacante remoto no autenticado puede enviar una solicitud HTTP especialmente diseñada para realizar una inyección de OData y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación. La explotación exitosa de esta vulnerabilidad puede permitir a un atacante remoto leer, eliminar, modificar datos en la base de datos y obtener control total sobre la aplicación afectada.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-33612 de tipo validación de certificado inadecuada, podría permitir a un atacante remoto realizar un ataque MitM. La vulnerabilidad existe debido a una validación de certificado incorrecta. Un atacante remoto puede hacerse pasar por un sistema de proveedor de instancias y realizar un ataque MitM.

A. Productos afectados:

- BIG-IP Next Central Manager: 20.0.1 - 20.1.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://my.f5.com/manage/s/article/K000139012

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°108	Fecha: 09-05-2024
		Página: 6 de 7

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en el protocolo AVDTP Bluetooth de Microsoft Windows		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo desbordamiento de enteros en el protocolo AVDTP Bluetooth de Microsoft Windows. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de Microsoft Windows.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-24948 de tipo desbordamiento de enteros, podría permitir a un atacante adyacente a la red ejecutar código arbitrario en instalaciones afectadas de Microsoft Windows. Se requiere la interacción del usuario para aprovechar esta vulnerabilidad, ya que el objetivo debe conectar un dispositivo Bluetooth malicioso. La falla específica existe en el procesamiento de paquetes AVDTP. El problema se debe a la falta de una validación adecuada de los datos proporcionados por el usuario, lo que puede provocar un desbordamiento insuficiente de enteros antes de escribir en la memoria. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del kernel.

Para aprovechar esta vulnerabilidad, la víctima debe emparejarse con el dispositivo Bluetooth del atacante. Un atacante autorizado podría aprovechar la vulnerabilidad del controlador Bluetooth de Windows ejecutando mediante programación ciertas funciones que podrían conducir a la elevación de privilegios en el componente Bluetooth. Un atacante que aprovechara con éxito esta vulnerabilidad podría obtener privilegios de SISTEMA.

A. Productos afectados:

Las siguientes versiones de Windows de 32bits, 64 bits y ARM64 afectadas por esta vulnerabilidad son:

- Windows 10 versión 1809, afectado desde 10.0.0 antes de 10.0.17763.4377.
- Servidor Windows 2019, afectado desde 10.0.0 0antes de 10.0.17763.4377.
- Windows 10 versión 20H2, afectado desde 10.0.0 antes de 10.0.19042.2965.
- Windows 11 versión 21H2, afectado desde 10.0.0 antes de 10.0.22000.1936.
- Windows 10 versión 21H2, afectado desde 10.0.0 antes de 10.0.19044.2965.
- Windows 10 versión 22H2, afectado desde 10.0.0 antes de 10.0.19045.2965.
- Windows 10 versión 1507, afectado desde 10.0.0 antes de 10.0.10240.19926.
- Windows 10 versión 1607, afectado desde 10.0.0 antes de 10.0.14393.5921.
- Servidor Windows 2016, afectado desde 10.0.0 antes de 10.0.14393.5921.
- Windows Server 2016 (instalación de Server Core), afectado desde 10.0.0 antes de 10.0.14393.5921.
- Servidor Windows 2012, afectado desde 6.2.0 anterior a 6.2.9200.24266.
- Windows Server 2012 (instalación de Server Core), afectado desde 6.2.0 anterior a 6.2.9200.24266.
- Servidor Windows 2012 R2, afectado desde 6.3.0 anterior a 6.3.9600.20969.
- Windows Server 2012 R2 (instalación de Server Core), afectado desde 6.3.0 anterior a 6.3.9600.20969.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24948 • hxxps://www.zerodayinitiative.com/advisories/ZDI-24-439/

Índice alfabético